# Section 04: Propositions and Proofs

## 1. Formal Proof (Direct Proof Rule)

Give a formal proof that $\neg t \to s$ follows from $t \lor q$, $q \to r$ and $r \to s$ with a formal proof. Then, translate your proof to English.

If you want to do your formal proof on Cozy. You can do so on this page.

## 2. Formal Proof

Give a formal proof that $\neg p$ follows from $\neg(\neg r \lor t)$, $\neg q \lor \neg s$ and $(p \to q) \land (r \to s)$ with a formal proof. Then, translate your proof to English.

If you want to do your formal proof on Cozy. You can do so on this page.

## 3. Spoof and Goofs

For each claim, translate the English proof into a formal proof and say whether it is a **spoof** (the claim is true but the proof is wrong) or a **goof** (the claim is false). Then, if it is a spoof, point out the errors in the proof and explain how to correct them, and if it is a goof, point out the first error and show that the claim is false by giving a counterexample.

(a) Show that $r$ follows from $\neg p$ and $p \leftrightarrow r$.

*Spoof:* Since we are given that $p \leftrightarrow r$, we know $p \to r$. We are also given that $\neg p$ holds, so it must be the case that $\neg p \lor (p \lor r)$ holds. This claim is equivalent to $(p \land \neg p) \to r$. Since this last claim starts by assuming both $p$ and $\neg p$, we can infer that this holds with just $\neg p$, giving us $\neg p \to r$. Since we were given that $\neg p$ holds, we get that $r$ holds.

(b) Show that $\exists z\, \forall x\, P(x, z)$ follows from $\forall x\, \exists y\, P(x, y)$.

*Spoof:* We are given that, for every x, there is some y such that P(x, y) holds. Thus, there must be some object c such that for every x, P(x, c) holds. This shows that there exists an object z such that, for every x, P(x, z) holds.

(c) Show that $\exists z\, (P(z) \land Q(z))$ follows from $\forall x\, P(x)$ and $\exists y\, Q(y)$.

*Spoof:* Let z be arbitrary. Since we were given that for every x, P(x) holds, P(z) must hold. Since we were given that there is a y such that Q(y) holds, Q(z) must also hold. From the previous facts, we know that there is some object z such that P(z) and Q(z) hold.

## 4. Predicate Logic Formal Proof

Given $\forall x\, T(x) \to M(x)$, we wish to prove $(\exists x\, T(x)) \to (\exists y\, M(y))$.

The following formal proof does this, but it is missing explanations for each line. Fill in the blanks with inference rules or equivalences to apply (as well as the line numbers) to complete the proof. Then, translate the proof to English.

1. $\forall x\, T(x) \to M(x)$ (________________)

    2.1. $\exists x\, T(x)$ (________________)
    2.2. $T(c)$ (________________)
    2.3. $T(c) \to M(c)$ (________________)
    2.4. $M(c)$ (________________)
    2.5. $\exists y\, M(y)$ (________________)

2. $(\exists x\, T(x)) \to (\exists y\, M(y))$ (________________)

## 5. A Formal Proof in Predicate Logic

Give a formal proof that $\exists x\ (P(x) \vee R(x))$ follows from $\forall x\ (P(x) \vee Q(x))$ and $\forall y\ (\neg Q(y) \vee R(y))$. Then, translate your proof to English.

If it helps, in your proof, you can assume that "a" is the name of a well-known constant in this domain (like $\pi$ is in the domain of real numbers).

If you want to do your formal proof on Cozy. You can do so on this page.

## 6. Prime Checking

You wrote the following code, `isPrime(int n)` which you are confident returns `true` if and only if $n$ is prime (we assume its input is always positive).

```
public boolean isPrime(int n) {
    int potentialDiv = 2;
    while (potentialDiv < n) {
        if (n % potenttialDiv == 0)
            return false;
        potentialDiv++;
    }
    return true;
}
```

Your friend suggests replacing `potentialDiv < n` with `potentialDiv <= Math.sqrt(n)`. In this problem, you'll argue the change is ok. That is, your method still produces the correct result if $n$ is a positive integer.

We will use "nontrivial divisor" to mean a factor that isn't 1 or the number itself. Formally, a positive integer $k$ being a "nontrivial divisor" of $n$ means that $k|n$, $k \neq 1$ and $k \neq n$. Claim: when a positive integer $n$ has a nontrivial divisor, it has a nontrivial divisor at most $\sqrt{n}$.

(a) Let's try to break down the claim and understand it through examples. Show an example (a specific $n$ and $k$) of a nontrivial divisor, of a divisor that is not nontrivial, and of a number with only trivial divisors.

(b) Prove the claim. Hint: you may want to divide into two cases!

(c) Informally explain why the fact about integers proved in (b) lets you change the code safely.